# EAST Search History

| Ref # | Hits | Search Query | DBs | Default Operator | Plurals | Time Stamp |
|---|---|---|---|---|---|---|
| S1 | 2 | ("20050066186").PN. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2007/12/05 21:03 |
| S2 | 0 | ("2005/0066186").URPN. | USPAT | OR | ON | 2007/12/05 21:04 |
| S3 | 2 | (GENTLE, CHRISTOPHER REON).in. | USPAT | AND | ON | 2007/12/05 21:04 |
| S4 | 1 | (ORBACH, JULIAN JAMES ).in. | USPAT | AND | ON | 2007/12/05 21:05 |
| S5 | 2057 | (713/193).CCLS. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2007/12/05 21:05 |
| S6 | 467 | (713/167).CCLS. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2007/12/05 21:05 |
| S7 | 2462 | S5 S6 | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:05 |
| S8 | 1699 | S7 and @ad<"20030920" | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:10 |
| S9 | 96 | S8 and (keyboard same encrypt$5) | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:24 |
| S10 | 254 | (encrypt$3 with (keyboard or keypad or typed) with (seed or pin)) | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:24 |
| S11 | 4 | enter$3 with encryption$ with seed with (keypad or keyboard) | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:24 |
| S12 | 414 | enter$3 with encrypt$3 with (keypad or keyboard) | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:25 |

# EAST Search History

| | | | | | | |
|---|---|---|---|---|---|---|
| S13 | 287 | S12 and @ad<"20030920" | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:26 |
| S14 | 38 | S8 and (encrypt$3 with (keyboard or keypad or typed)) | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:26 |
| S15 | 1374 | encrypt$3 with (keyboard or keypad) | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:26 |
| S16 | 902 | S15 and @ad<"20030920" | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:26 |
| S17 | 28 | encrypt$3 with (keyboard or keypad) with seed | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:27 |
| S18 | 17 | S17 and @ad<"20030920" | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:27 |
| S19 | 228 | encrypt$3 with (keyboard or keypad) with pin | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:27 |
| S20 | 152 | S19 and @ad<"20030920" | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | OR | ON | 2007/12/05 21:27 |

INTERFERENCE SEARCH

# EAST Search History

| Ref # | Hits | Search Query | DBs | Default Operator | Plurals | Time Stamp |
|---|---|---|---|---|---|---|
| S2 | 4 | (keyboard encrypt$3 device seed transmit$4 read$3).clm. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | AND | ON | 2007/12/05 21:29 |
| S3 | 4 | (keyboard encrypt$3 device seed transmit$4 read$3 generat$3).clm. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | AND | ON | 2007/12/05 21:30 |
| S4 | 1 | (keyboard encrypt$3 device seed transmit$4 read$3 protect$3).clm. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | AND | ON | 2007/12/05 21:30 |
| S5 | 5 | (keyboard encrypt$3 device seed transmit$4).clm. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | AND | ON | 2007/12/05 21:34 |
| S6 | 2 | (keypad keyboard number key start signal stop).clm. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | AND | ON | 2007/12/05 21:34 |
| S8 | 1 | (transmission keyboard encrypt$3 link interface memory keypad routine).clm. | US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB | AND | ON | 2007/12/05 21:35 |

Terms used: **keyboard** and **encryption seed** and **device** and **reader** and **keypad** and **encrypting** and **transmitting**

Found **5,929** of **215,737**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Macintosh human interface guidelines

Apple Computer, Inc.
January 1992 Book

**Publisher:** Addison-Wesley Publishing Company

Full text available: pdf(37.61 MB) Additional Information: full citation, abstract, references, cited by, index terms

Macintosh Human Interface Guidelines describes the way to create products that optimize the interaction between people and Macintosh computers. It explains the whys and hows of the Macintosh interface in general terms and specific details.

Macintosh Human Interface Guidelines helps you link the philosophy behind the Macintosh interface to the actual implementation of interface elements. Examples from a wide range of Macintosh products show good human interface design, including individ ...

2 User interfaces and UI design: BlueTable: connecting wireless mobile devices on interactive surfaces using vision-based handshaking

Andrew D. Wilson, Raman Sarin
May 2007 **Proceedings of Graphics Interface 2007 GI '07**

**Publisher:** ACM Press

Full text available: pdf(1.96 MB) Additional Information: full citation, abstract, references, index terms

Associating and connecting mobile devices for the wireless transfer of data is often a cumbersome process. We present a technique of associating a mobile device to an interactive surface using a combination of computer vision and Bluetooth technologies. Users establish the connection of a mobile device to the system by simply placing the device on a table surface. When the computer vision process detects a phone-like object on the surface, the system follows a handshaking procedure using Blue ...

**Keywords**: bluetooth, computer vision, interactive tabletops, mobile devices, ubiquitous computing

3 Privacy and access control: Lessons learned from the deployment of a smartphone-based access-control system

Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter, Kami Vaniea
July 2007 **Proceedings of the 3rd symposium on Usable privacy and security SOUPS**

'07

**Publisher:** ACM Press

Full text available: pdf(920.64 KB) Additional Information: full citation, abstract, references, index terms

Grey is a smartphone-based system by which a user can exercise her authority to gain access to rooms in our university building, and by which she can delegate that authority to other users. We present findings from a trial of Grey, with emphasis on how common usability principles manifest themselves in a smartphone-based security application. In particular, we demonstrate aspects of the system that gave rise to failures, misunderstandings, misperceptions, and unintended uses; network effects ...

**Keywords**: access control, mobile computing, security, smartphones, usability

4 Technical reports

SIGACT News Staff

January 1980 **ACM SIGACT News**, Volume 12 Issue 1

**Publisher:** ACM Press

Full text available: pdf(5.28 MB) Additional Information: full citation

5 Information leakage from optical emanations

Joe Loughry, David A. Umphress

August 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 3

**Publisher:** ACM Press

Full text available: pdf(382.77 KB) Additional Information: full citation, abstract, references, index terms

A previously unknown form of compromising emanations has been discovered. LED status indicators on data communication equipment, under certain conditions, are shown to carry a modulated optical signal that is significantly correlated with information being processed by the device. Physical access is not required; the attacker gains access to all data going through the device, including plaintext in the case of data encryption systems. Experiments show that it is possible to intercept data under ...

**Keywords**: COMINT, COMSEC, EMSEC, SIGINT, TEMPEST, communication, compromising emanations, covert channel, encryption, fiber optics, information displays, light emitting diode (LED)

6 Shake 'em, but don't crack 'em: Shake them up!: a movement-based pairing protocol for CPU-constrained devices

Claude Castelluccia, Pars Mutaf

June 2005 **Proceedings of the 3rd international conference on Mobile systems, applications, and services MobiSys '05**

**Publisher:** ACM Press

Full text available: pdf(295.02 KB) Additional Information: full citation, abstract, references, cited by, index terms

This paper presents a new pairing protocol that allows two CPU-constrained wireless devices Alice and Bob to establish a shared secret at a very low cost. To our knowledge, this is the first software pairing scheme that does not rely on expensive public-key cryptography, out-of-band channels (such as a keyboard or a display) or specific hardware, making it inexpensive and suitable for CPU-constrained devices such as sensors.

In the described protocol, Alice can send the secre ...

7 Pen computing: a technology overview and a vision

André Meyer
July 1995 **ACM SIGCHI Bulletin**, Volume 27 Issue 3
**Publisher:** ACM Press
Full text available: pdf(5.14 MB) Additional Information: full citation, abstract, citings, index terms

This work gives an overview of a new technology that is attracting growing interest in public as well as in the computer industry itself. The visible difference from other technologies is in the use of a pen or pencil as the primary means of interaction between a user and a machine, picking up the familiar pen and paper interface metaphor. From this follows a set of consequences that will be analyzed and put into context with other emerging technologies and visions.Starting with a short historic ...

8 Papers from MC²R open call: Using visual tags to bypass Bluetooth device discovery

David Scott, Richard Sharp, Anil Madhavapeddy, Eben Upton
January 2005 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 9 Issue 1
**Publisher:** ACM Press
Full text available: pdf(311.14 KB) Additional Information: full citation, abstract, references, citings, index terms

One factor that has limited the use of Bluetooth as a networking technology for publicly accessible mobile services is the way in which it handles Device Discovery. Establishing a Bluetooth connection between two devices that have not seen each other before is slow and, from a usability perspective, often awkward. In this paper we present the implementation of an end-to-end Bluetooth-based mobile service framework designed specifically to address this issue. Rather than using the standard Blueto ...

9 Objective and alternatives for a computer assisted instruction system for the visually handicapped

William L. Ballenger
June 1979 **ACM SIGLASH Newsletter**, Volume 12 Issue 2
**Publisher:** ACM Press
Full text available: pdf(3.10 MB) Additional Information: full citation, abstract, references

In computer assisted instruction (CAI), a dialogue of information can be maintained between the computer and a learner without dependence upon normal vision. This is possible because there are several media alternatives for information input to the learner. These alternatives include large print (visual), braille (tactile), the OPTACON reading system (tactile), and auding (auditory). The criteria used to evaluate each medium for information input include the percentage of the visually handicappe ...

10 Model for non-expert text entry speed on 12-button phone keypads

Andriy Pavlovych, Wolfgang Stuerzlinger
April 2004 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '04**
**Publisher:** ACM Press
Full text available: pdf(362.45 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we present a new model for predicting text entry speed on a 12-button mobile phone keypad. The proposed model can predict the performance of novice users. Like other models for text entry, the proposed model includes a movement component based on Fitts' law and a linguistic component based on letter digraph probabilities. It also adds cognitive delay times before key presses and takes into account the fact that Fitts'

law cannot model multiple presses of the same key accurately. Fi ...

**Keywords**: mobile phones, model, text entry

11 A structural view of the Cedar programming environment

Daniel C. Swinehart, Polle T. Zellweger, Richard J. Beach, Robert B. Hagmann
August 1986 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 8 Issue 4
**Publisher:** ACM Press

Full text available: pdf(6.32 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents an overview of the Cedar programming environment, focusing on its overall structure—that is, the major components of Cedar and the way they are organized. Cedar supports the development of programs written in a single programming language, also called Cedar. Its primary purpose is to increase the productivity of programmers whose activities include experimental programming and the development of prototype software systems for a high-performance personal computer. T ...

12 Authentication: Pass-thoughts: authenticating with our minds

Julie Thorpe, P. C. van Oorschot, Anil Somayaji
September 2005 **Proceedings of the 2005 workshop on New security paradigms NSPW '05**
**Publisher:** ACM Press

Full text available: pdf(3.94 MB) Additional Information: full citation, abstract, references

We present a novel idea for user authentication that we call *pass-thoughts*. Recent advances in Brain-Computer Interface (BCI) technology indicate that there is potential for a new type of human-computer interaction: a user transmitting thoughts directly to a computer. The goal of a pass-thought system would be to extract as much entropy as possible from a user's brain signals upon "transmitting" a thought. Provided that these brain signals can be recorded and processed in an accurate and ...

**Keywords**: authentication, passwords

13 Symmetric and Asymmetric Encryption

Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
**Publisher:** ACM Press

Full text available: pdf(2.23 MB) Additional Information: full citation, references, citings, index terms

14 Security on the move: indirect authentication using Kerberos

Armando Fox, Steven D. Gribble
November 1996 **Proceedings of the 2nd annual international conference on Mobile computing and networking MobiCom '96**
**Publisher:** ACM Press

Full text available: pdf(1.34 MB) Additional Information: full citation, references, citings, index terms

15 Passwords: Reducing shoulder-surfing by using gaze-based password entry

Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd
July 2007 **Proceedings of the 3rd symposium on Usable privacy and security SOUPS**

'07
**Publisher:** ACM Press
Full text available: pdf(241.05 KB) Additional Information: full citation, abstract, references, index terms

Shoulder-surfing -- using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information -- is a problem that has been difficult to overcome. When a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. We present EyePassword, a system that mitigates the issues of shoulder surfing via a novel approach to ...

**Keywords**: eye tracking, gaze-based password entry, password entry, shoulder surfing

16 Protecting applications with transient authentication
Mark D. Corner, Brian D. Noble
May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**
**Publisher:** ACM Press
Full text available: pdf(294.40 KB) Additional Information: full citation, abstract, references, cited by

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

17 Geographic Data Processing
George Nagy, Sharad Wagle
June 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 2
**Publisher:** ACM Press
Full text available: pdf(4.20 MB) Additional Information: full citation, references, citings, index terms

18 Some cryptographic principles of authentication in electronic funds transfer systems
C. H. Meyer, S. M. Matyas
October 1981 **ACM SIGCOMM Computer Communication Review , Proceedings of the seventh symposium on Data communications SIGCOMM '81**, Volume 11 Issue 4
**Publisher:** ACM Press
Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, citings, index terms

One essential requirement of an Electronic Funds Transfer (EFT) system is that institutions must be able to join together in a common EFT network such that a member of one institution can initiate transactions at entry points in the domain of another institution. The use of such a network is defined as interchange. Cryptographic implementations are developed for such a network in such a way as to keep personal verification and message authentication processes at diffe ...

19 Utilities: Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes
Cynthia Kuo, Mark Luk, Rohit Negi, Adrian Perrig
November 2007 **Proceedings of the 5th international conference on Embedded networked sensor systems SenSys '07**

**Publisher:** ACM
Full text available: pdf(372.06 KB) Additional Information: full citation, abstract, references, index terms

Existing protocols for secure key establishment all rely on an unspecified mechanism for initially deploying secrets to sensor nodes. However, no commercially viable *and* secure mechanism exists for initial setup. Without a guarantee of secure key deployment, the traffic over a sensor network cannot be presumed secure.

To address this problem, we present a user-friendly protocol for the secure deployment of cryptographic keys in sensor networks. We propose a collection of five te ...

**Keywords**: Faraday cage, human error, key deployment, sensor network, wireless communication

20 Access to graphical interfaces for blind users

W. Keith Edwards, Elizabeth D. Mynatt, Kathryn Stockton
January 1995 **interactions**, Volume 2 Issue 1
**Publisher:** ACM Press
Full text available: pdf(1.76 MB) Additional Information: full citation, references, citings, index terms, review

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next